A Hybrid Regression-Based Network Model for Continuous Face Recognition and Authentication

Bhanu Kiran Devisetty*, Ayush Goyal, Avdesh Mishra, Mais W Nijim, David Hicks, George Toscano
Department of Electrical Engineering and Computer Science, Texas A&M University-Kingsville, Kingsville, Texas

***Abstract*—This research proposes a continuous remote biometric user authentication system implemented with a face recognition model pre-trained on face images. This work develops an algorithm combining the Hybrid Block Overlapping KT Polynomials (HBKT) and Regression-based Support Vector Machine (RSVM) methods for a face recognition-based remote user authentication system that uses a model pre-trained on the ORL, Face94 and GT datasets to recognize authorized users from face images captured through a webcam for continuous remote biometric user authentication. HBKT polynomials enhance feature extraction by capturing local and global facial patterns, while RSVM improves classification performance through efficient regression-based decision boundaries. The system can continuously capture user face images from the user's webcam for user authentication, but it can be affected by lighting variations, occlusion, and computational overhead from continuous image capture. This has been implemented in a Python program. The proposed method, when compared to previous state-of-the-art algorithms, was observed to have higher F-measure, accuracy, and speed, for most of the cases. The proposed method was observed to have accuracies of 98.82% (ORL dataset), 96.73% (GT dataset), and 95.9% (Face94 dataset).**

***Keywords*—Vision-based computing; object detection; face detection; face recognition; feature extraction; feature coefficients; classification; authentication; biometrics; biometric authentication**

I. INTRODUCTION

Before allowing a user access to a secured location, resource, or system, authentication confirms the user's identity using specific credentials. Generally speaking, authentication only occurs during the user's initial interaction with the system [1]. Under these circumstances, the user is prompted with knowledge-based authentication that resembles password inquiry. The author is deemed authenticated if the user correctly replies with an example password [2]. However, one-time authentication is the standard for authentication; researchers have examined a variety of concerns, including security flaws and user dissatisfaction. For instance, when trying to unlock a smartphone with a pattern- or password-based authentication system, the user must concentrate on multiple authentication processes [3]. Driving while distracted is one concern that could arise from this for user safety. One-time authentication's lack of ability to identify attackers after the initial authentication is a significant security vulnerability [4]. For instance, if an authorized user forgets to log out or leaves their authenticated device unattended, an unauthorized user may be able to access their private resources. The above mentioned issues have prompted research into continuous authentication techniques [5]. To ensure the person who used the device to authenticate themselves the first time is still using it, these methods keep an eye on how the user interacts with it even after logging in. Simple security measures that lock users' devices and require them to re-enter their passwords after a certain amount of inactivity served as the foundation for the first attempts in this approach [6]. Though there is potential for improvement, such systems may upset people while they present a window of vulnerability. There are significant increases in the research literature on using behavior metrics, such as keystroke frequency, and biometrics, such as facial features, for continuous authentication [7]. This field has seen rapid growth, as evidenced by the numerous publications in the last ten years.

Researchers' interest in wearable medical sensors (WMSs) has grown, and these devices are beginning to be used in clinical settings. These sensors measure biological data, such as body temperature, blood pressure, and heart rate. The sales of 33 million wearable health monitoring gadgets, according to a recent Business Insider piece, are also analyzed [8]. According to the forecast, this number will rise quickly after reaching 148 million in 2019. The author proposes that such biomedical signals can also be utilized to provide authentication since they will be gathered in any case for health monitoring purposes [9]. Three factors make using biological data continuously collected for user identification and verification seem promising [10]. First, there is no need for an additional device on the body to use biological signals for authentication if WMSs are already gathering them for medical purposes. Secondly, the user is not heavily involved in collecting this data, as it is done transparently. In contrast to conventional biometrics and behavior metrics such as facial features and keyboard patterns, which may sometimes become unavailable, the biomedical signal stream obtained from wearable medical devices (WMSs) remains accessible as long as the user wears them [11] – [15]. The challenges encountered in the existing approaches are resolved using the anticipated model discussed below:

The transparent continuous authentication system H-RSVM is presented in this paper. It is based on a set of facial images provided to validate the user's authenticity. It is generally called the face recognition process. Image samples are continuously collected from the available online resources for diagnostic and therapeutic reasons. The primary distinction between a biometric characteristic and an input image is that the latter lacks the necessary discriminatory capacity to identify individuals independently. Therefore, it is doubtful that an authentication decision based solely on facial images will be adequately discriminative. Still, integrating many image samples into a single framework makes for a powerful continuous authentication mechanism. This study improves the biometric

remote authentication using HBKT polynomials integrated with RSVM, and makes it faster and more accurate than earlier studies. It affords a smooth, uninterrupted user authentication through the actual capture of images by webcams for real time and non-intrusive authentication. The proposed method is very stable and optimized for use in applications like secure remote authentication. The following sums up our primary accomplishments:

1) For the design of any continuous authentication system, this work proposes a novel H-RSVM where the features from the image datasets are analyzed and classified to have better prediction accuracy.

2) To assess the ability of prediction and to differentiate individuals, these works propose implementing a continuous authentication system known as H-RSVM and analyzing its accuracy and scalability.

3) We present a method for adaptive authorization and discuss its potential application in resolving challenges faced by users due to possible erroneous restrictions imposed by continuous authentication systems. This work outlines several potential defences against the suggested continuous authentication method and many ways to avoid them.

The work is structured as follows: Section II gives an extensive analysis of various prevailing approaches used for authentication during face recognition. Section IV delves into the problem statement. The methodology is elaborated in Section IV. The numerical outcomes are discussed in Section V, and work summarization is provided in Section VI.

II. Literature Review

It has been suggested in numerous research studies that biometrics be used for ongoing user authentication. In real-time authentication, inertial data demonstrates location, movement and device orientation concerning its surroundings [16]. Based on user activity, nonintrusive authentication techniques utilize this data to generate behavioral characteristics, such as voice, hand gestures, keyboard patterns, locomotion, touchscreen operations, and signature movements. Yu et al. [17] were the first to use a one-class distance-based classifier and build a sizable dataset for continuous authentication. They combined touchscreen, pressure, acceleration, time interval, and touch area size data with inertial data from the device's gyroscope and accelerometer. Their objective was to discern the authenticity of smartphone users, distinguishing between genuine and fraudulent individuals [18]. By generating research profiles, they achieved an Equal Error Rate (EER) of up to 3.6%, which varied depending on how each user held their device while entering their Personal Identification Number (PIN). By examining keyboard and handwriting data gathered from password submissions, Sun et al. [19] validated smartphone users in their study using deep learning techniques. The researchers categorized the images using various models, such as Naïve Bayes, Bayesian Net classifiers, and multilayer perceptrons (MLP) [20].

In a subsequent study, Menotti et al. [21] utilized a comprehensive dataset from Google's Abacus project, employing advanced techniques such as time-based deep feature extraction. Their research's main goal was to develop user authentication, and they did so by using recurrent and convolutional neural networks (CNNs and RNNs, respectively). The Google Abacus dataset, which includes 1500 people's information in their natural settings, was used for this. It is crucial to remember that this dataset is not publicly accessible. The researchers used the D-RNN model to categorize the data. Qin et al. [22] used the HMOG dataset, which included more than 27,000 samples from 10 participants, to show notable progress in the field. Wavelet, frequency, and time domain features were used to test algorithms like SVM, K-Nearest Neighbors and Hidden Markov Models. Based on an adaptation of Zhu et al. [23], speech, keyboards, touchscreens, gestures, handwriting, and mobility have all been studied in research. The requirement for user input during the whole authentication procedure is the primary disadvantage of gesture-based research [24]. It is impossible to identify an unauthorized user after the device is unlocked. However, compared to other methods, keystroke dynamics solutions are more constrained and require more data since they are impacted by fluctuations in user behavior, such as moods [25].

Moreover, changing keyboards may cause previously taught actions to become erratic. Additional research constraints conducted using touchscreens include the variability of interactions based on the device's orientation and the influence of user behavior on the level of interactivity [26]. Handwriting-based methods are seldom designed to support continuous authentication due to the smartphone's inability to detect pattern changes accurately. Speech-based authentication technologies are also hindered by background noise from the surrounding environment [27]. Furthermore, gait-based recognition, which relies on maintaining consistent positioning of the body's sensors, is vulnerable to modifications in walking patterns resulting from adjustments in clothing. Various projects have been dedicated to verifying human actions in a specific work context, such as retrieving a phone from a surface, initiating a phone call, or inputting a password [28]. While a more straightforward machine learning problem might yield better outcomes, it needs more consistency. For instance, the phone only knows how to classify various behaviors once the same activity is performed frequently once a user has been granted permission. Two different user activities are detectable by motion sensors. While the second is complex, the first is easy. Simple activities include sitting, sleeping, walking, climbing and descending stairs, and lying down [29]. In contrast, complex tasks involve riding a bike, exercising, changing clothes, and operating a vehicle. A method for determining when people are driving, biking, walking, using the bus, or utilizing the train in real time was created by Vijaya et al. [30]. This technique makes use of accelerometer and GPS data. They demonstrated that GPS data processed using principal component analysis (PCA) and recursive feature elimination (RFE) in conjunction with a random forest (RF) classifier yielded 96% accuracy. However, because GPS requires user clearance to access data and has high battery consumption, its usage in CA contexts is not practicable for real-world deployment. Support vector machine (SVM) models using accelerometer and gyroscope data were developed [30]. The model they developed was able to identify 95% of the different walking patterns, including going upwards (79%), standing (92%), sitting (94%), lying down (100%), and climbing

stairs (72%) [31] – [35]. Similar methods were used to investigate human activity detection with artificial neural networks and deep learning, yielding a 95% accuracy rate.

III. PROBLEM STATEMENT

The challenge in continuous user authentication is to create effective and non-intrusive method to distinguish between genuine and fraudulent users in various real-world conditions. Existing methods such as Gesture based, keystroke dynamics, and speech-based authentication continue to face challenges of variation, noise or changes in orientation thus producing varying results. Further, gait-based recognition is vulnerable to cloth variation or change of body posture whereas the GPS based systems though very accurate are not feasible due their high-power consumption and privacy issue. Thus, the problem is to develop a continuous authentication framework that combines multiple behavioral and biometric data and real-time authentication with minimal user input. The proposed method provides better optimal accuracy and flexibility by utilizing combined behavioral parameters and biometrics to enhance security to particular contexts of use without compromising the convenience of the end-users.

IV. METHODOLOGY

Face recognition is required in various applications, and significant progress has been identified in this research. The proposed work of remote user access with face verification consists of the following stages. Samples of face images from databases and the overall architecture are shown and discussed.

A. Dataset

The 400 grey-scale pictures in the AT&T database, once called "The ORL Database of Faces," feature 40 subjects [36-37]. Each issue has ten pictures that include every potential combination of attributes. Each subject's face samples are provided in the Portable Gray Map (PGM) format. Fig. 1 displays a variety of face samples from the databases that are utilized for training the model used in this work.

B. Pre-processing

It is the most widely utilized method for completing pre-processing. It changes the values in the image to fall between 0 and 1. Zero means and z-score normalization are the normalization techniques taken into consideration here, as stated in the equation below:

$$X_i' = \frac{X_i - mean\ (X)}{SD\ (X)} \tag{1}$$

In this case, the symbol X_i' represents data that has been normalized. The average value of the input X is represented by the mean (X), and the SD (X) represents the standard deviation. The equation below gives the expression for computing standard deviation:

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left(X_i - mean\ (X)\right)^2} \tag{2}$$

In this case, the provided input values' standard deviation is indicated as σ.

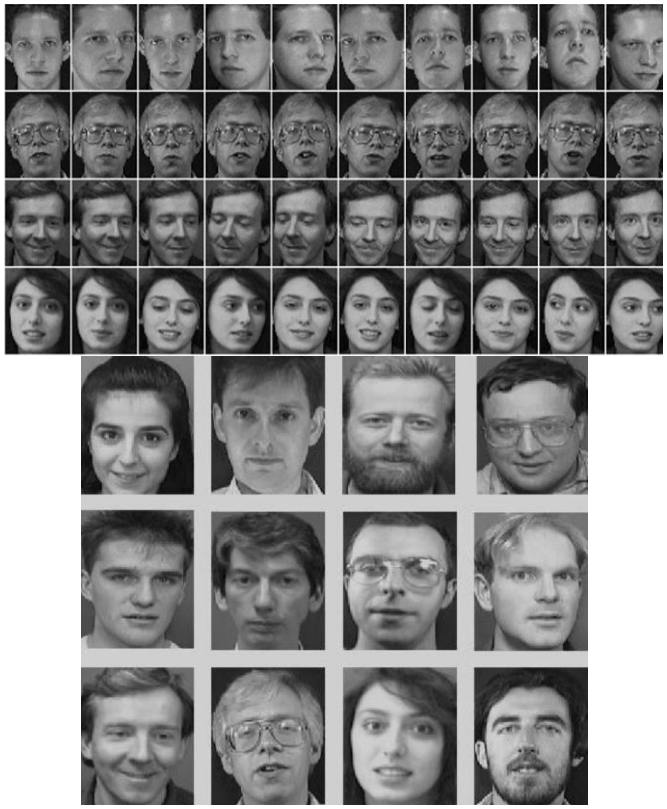

Fig. 1. Samples from the face image databases [36-37].

C. Feature Extraction

The weighted and normalized Krawtchouk polynomial's nth order is defined in the equation below as follows:

$$K_n\ (x; p, N-1) = \sqrt{\frac{\omega_K(x)}{\rho_K}}\, F_1\left(-n, -x;\ -N+1;\ \frac{1}{p}\right)$$

$$\text{where, } n, x = 0,1, \ldots, N-1;\ p \in (0,1) \tag{3}$$

Fig. 2 shows the overall architecture and functionality of the proposed work, which includes both feature extraction using HBKT polynomials and face recognition using RSVM.

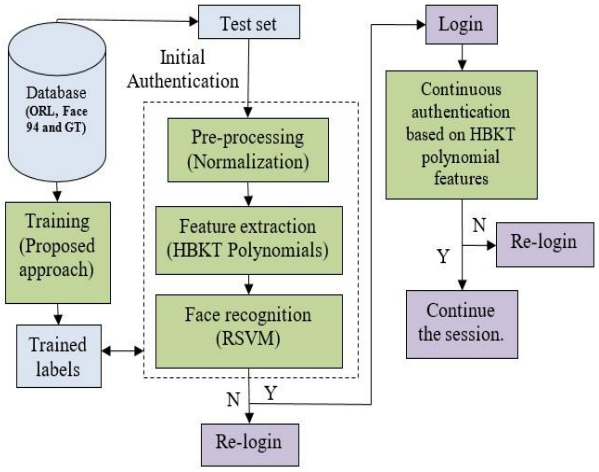

Fig. 2. Overall architecture of proposed work.

The norm and weight functions of the KP, denoted by ρ_K and ω_K, have been defined in the following manner:

$$\omega_K(x) = \binom{N-1}{x} p^x (1-p)^{N-x-1} \quad (4)$$

$$\rho_K(n) = (-1)^n \binom{1-p}{p}^n \frac{n!}{(-N+1)_n} \quad (5)$$

The three-term recurrence method is utilized to estimate KP coefficients since it is more computationally expensive to calculate KP coefficient values employing gamma and hypergeometric functions. Numerous studies have looked into this strategy. The author offered initial recurrence relation in n −direction and established recurrence relation. The recurrence relations divide the n- x plane into two regions. One of these regions has its KP coefficients computed, while the other region's coefficients are derived using a symmetry relation.

The author suggested using a dual n −direction recurrence relation involving forward and backward computations to find new KP coefficients. KP plane comprises four triangular sections for which coefficients are determined for two of the triangles. In contrast, the remaining two triangles' coefficients are derived using symmetry relation. To compute KP coefficients, a rapid recurrence relation was recently developed. As shown in Fig. 3, this entails partitioning KP space into sections designated by both primary and secondary diagonals.

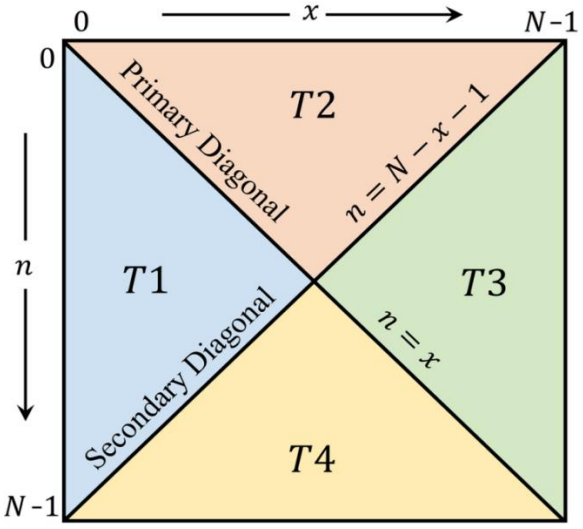

Fig. 3. KP plane.

For a wide range of parameters p, this method was better regarding computing speed, accuracy, and handling large signal quantities. In light of this rationale, the algorithm proposed is examined in this investigation. The procedure for computing the KP coefficients, denoted as $K_n(x;\ p, N-1)$ for brevity, is outlined in Fig. 4 (hereafter referred to as $K_n(x)$).

1) First, we compute $K_n(0)$ and $K_n(1)$ as follows:

$$K_n(0) = \sqrt{\frac{(N-n)p}{n(1-p)} * K_{n-1}(0)} \quad (6)$$

$$K_n(1) = \frac{-n+p(N-1)}{p(N-1)} \sqrt{\frac{(N-1)p}{(1-p)}} K_n(0) \quad (7)$$

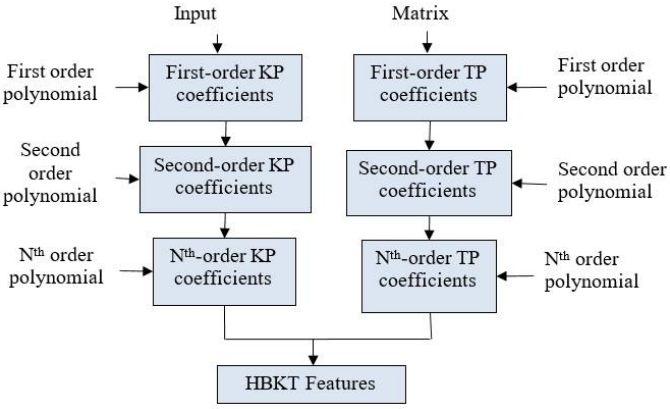

Fig. 4. HBKT feature extraction.

2) The recurrence relation in $the\ n$ direction can be used to determine KP coefficients within the temperature range T1.

$$\gamma_1 K_n(x+1) = \gamma_2 K_n(x) + \gamma_3 K_n(x-1) \quad (8)$$

$$\gamma_1 = \sqrt{p(N-x-1)(1-p)(x-1)} \quad (9)$$

$$\gamma_2 = -n + p(N-x-1) + x(1-p) \quad (10)$$

$$\gamma_3 = \sqrt{x(1-p)p(N-x)} \quad (11)$$

3) Using the symmetry connection about the main diagonal at n = x, the coefficients within the temperature range T2 can be found.

$$K_n(x) = K_x(n) \quad (12)$$

4) The symmetry relation concerning the secondary diagonal at $n = N - x - 1$ can be used to find the coefficients inside the temperature ranges T3 and T4.

$$K_{N-x-1}(x) = (-1)^{N-n-x-1} K_n(x) \quad (13)$$

5) The KP coefficients for p more significant than 0.5 values are computed using the equation below.

$$K_n(x: 1-p) = (-1)^n K_n(N-x-1; p) \quad (14)$$

D. Tchebichef Polynomial

The weighted and normalized TP's n^{th} order can be defined as follows:

$$T_n(x) = \sqrt{\frac{\omega_T(x)}{\rho_T(n)}} (1-N)_n F_2(-n, -x, 1+n; 1-N; 1), n, x = 0,1,\dots,N-1 \quad (15)$$

This formulation involves the weight function of the TP, represented as $\omega_T(x)$, and the squared norm of the TP, described as $\rho_T(n)$.

$$\omega_T(x) = 1 \quad (16)$$

$$\rho_T(n) = (2n)! \binom{N+n}{2n+1} \quad (17)$$

These are the definitions of these quantities. $\frac{a!}{b!(a-b)!}, F_2$ specifies the binomial coefficients, while $3F_2$ represents the hyper-geometric function:

$$3F_2\,(-n,-x,1+n;1,1-N;1)\;=\;\sum_{k=0}^{\infty}\frac{(-n)_k\,(-x)_k(1+n)_k}{(1)_k(1-N)_k k!} \quad (18)$$

$$(a)_k = a(a+1)(a+2).(a+k+1) \quad (19)$$

The computation of the rising factorial $(a)k$ can be determined by employing the three-term recurrence relation. This approach is precious in mitigating numerical instability and computational overload that may arise from using hyper-geometric and gamma functions for calculating TP coefficient values.

$$T_n\,(x) = \beta_1\,T_{n-1}\,(x) + \beta_2 T_{n-1}(x)$$

$$\text{Where } n = 2,3,\dots,N-1, x = 0,1,\dots,N-1 \quad (20)$$

With initial conditions:

$$T_0\,(x) = 1/\sqrt{N} \quad (21)$$

E. Krawtchouk and Tchebichef (KT) Polynomials

When features in the provided domain meet requirements for localization and EC attributes, managing elements becomes significantly easier. These capabilities greatly impact the processing stages as the signal can be described by characterizing its contents using a small number of moments. EC will reduce computational complexity because fewer moments must be computed to represent the signal fully. By identifying the region of interest (ROI), localization attribute in space provides further computational savings and facilitates feature categorization:

$$\mathbb{R}_n\,(x;N) = \sum_{j=0}^{N-1}\chi_j\,(x;p;N)\dot{y}_j(n;p,N) \quad (22)$$

$$n,x = 0,1,\dots,N-1 \quad (23)$$

To put it mathematically, the polynomial obtained by merging two OPs is also orthogonal. Combining two fundamental orthogonal polynomials, $Y_n(x;\,p,N)\;and\;X_n(x;\,p,N)$, yields the expression for the hybrid polynomial form $\mathbb{R}_n(x)$ at n^{th} order. The parameters defining these orthogonal polynomials denoted by p and N are built utilizing a particular combination level. The following are the formulas for $X_n(x;\,p,N)\;and\;Y_n(x;\,p,N)$.

$$\chi_n(x;p,N) = \sum_{i=0}^{N-1}K_i(n;p)T_j(x) \quad (24)$$

$$y_n(x;p,N) = \sum_{i=0}^{N-1}K_i(x;p)T_j(n) \quad (25)$$

$$n,x = 0,1,\dots,N-1;\; p\in(0,1)$$

The equation below can be used to express the suggested hybrid OP as follows:

$$R_n\,(x;p,N) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\sum_{l=0}^{N-1}K_j(i,p)T_j(x)K_l(n;p)T_l(i) \quad (26)$$

It is possible to express the equations using matrix notation. The polynomial forms of $R_n(x), X_n(x;\,p,N)$ $, Y_n(x;\,p,N), K_n(x), and\;T_n(x)$, respectively, correspond to the matrices $R, X, Y, R_k, and\;R_t$. In the equations below, it is demonstrated that the matrices KP and its transposition denoted as $R_k \equiv R_k^T$ are comparable. This significant observation highlights the symmetrical relationship between the KP coefficients along the major diagonal. Therefore, the related equations take on a particular form:

$$R = Y^T X \quad (27)$$

$$X = R_k^T R_t \quad (28)$$

$$Y = R_t^T R_k \quad (29)$$

$$R = (R_k R_t)^2 \quad (30)$$

In this context, the matrix transpose operator is denoted by $(\cdot)$. It is evident that $R_n(x)$ represents the squared expression of the sum of the Krawtchouk–Tchebichef polynomial (KP) and the Tchebichef polynomial (TP). Since the suggested set has a mathematical link with KP and TP, it can be represented by the squared Krawtchouk–Tchebichef polynomial (SKTP). Fig. 4 shows how the TP and KP modules generate the coefficients. It is noteworthy that, concerning KTP and TKP, SKTP has a notable localization characteristic and a higher EC property. Observing the SKTP coefficients symmetrically along the imaginary axis $x = (N-1)/2$ is possible. The SKTP coefficients of order $n = 127, 95, and\;64$ and those of order $n = 0, 31, and\;63$ are implied to correspond to this symmetry. In particular, $x = (N\,1)/2$ (imaginary axis), the SKTP coefficients range display symmetry are typically $n = \frac{N}{2}, \frac{N}{2}+1,\dots,N-1$. The values of $n = 0,1,\dots,N/2-1$ are included in these intervals. Moreover, the left half of the signal is associated with polynomial orders' coefficient within $n = 0,1,\dots,N/2-1$ range and the right half is related to the coefficients of polynomial orders within the range of $n = N/2, N/2+1,\dots,N-1$. Unlike TKP and KTP, where the indices of moments and signals are negatively correlated, the index of moments is linked to the indices of the signal in the signal domain. Furthermore, the SKTP basis functions for an $8*8$ block with diverse parameter p-values are shown in Fig. 3. The study reveals a gradual increase in low-frequency centre basis functions in vertical and horizontal orientations. The low frequency moves to the top left corner at a probability value of $p = 0.25$, as shown. Conversely, Fig. 3 illustrates that at a probability value of $p = 0.75$, the low frequency is displaced towards the lower right corner.

F. Regression-based Support Vector Machine (RSVM)

Support vector regression (SVR) was developed based on the support vector machine (SVM) methodology, primarily used for binary response variables. The fundamental concept behind SVR is constructing a tube with a width of ε around the data points, utilizing only residuals with absolute values more petite than a predetermined constant (referred to as ε-sensitivity). This concept is visually depicted in Fig. 5. In binary classification, two sets of points are established: those within a designated tube are not subject to penalties due to their proximity (within a predetermined threshold ε) to the predicted function. In contrast, those outside the tube are penalized based on their distance from the expected function. Support vector machines (SVMs) use a classification penalization strategy similar to this one. The methods of support vector machine learning (SVM) and support vector regression (SVR) rely on finding a hyper-plane that fits well in a feature space created by a kernel and can be efficiently generalized while maintaining the original features. Due to the scope of this book, an extensive examination of Support Vector

Regression (SVR) theory is not included. Whether SVR outperforms all other types of regression machines for continuous outcome prediction is also debatable. Because of this, we will now demonstrate how SVR is implemented in the e1071 library.

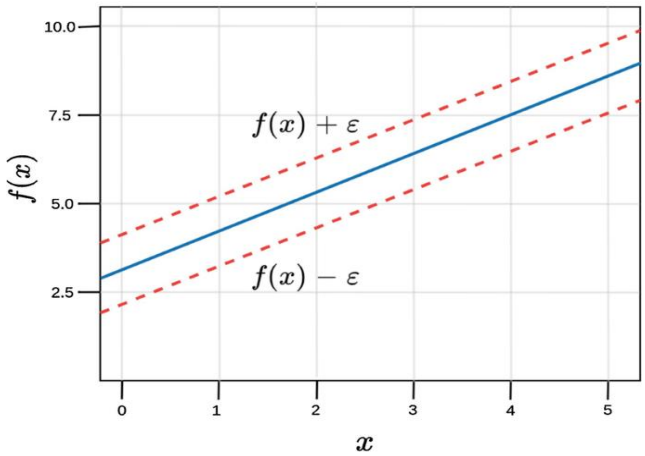

Fig. 5. Hyper-plane.

This part uses an FR system to evaluate the hybrid OP (SKTP) presented in terms of feature extraction. R-Support vector machines (SVM) are used in the facial recognition (FR) system's implementation. Fig. 5 shows the diagrammatic representation of the proposed method. The performance of KTP and TKP is evaluated against the hybrid OP, which can be generated using clear and noisy facial photographs within the FR system. The feature extraction process is the initial stage in the FR system. The image's height and width are extracted before any features are extracted using OP. We next use the given parameters, p and moment order, to generate the two polynomials, one for each dimension. Subsequently, the facial image is converted into the polynomial moment domain by applying the appropriate mathematical formula.

$$\Phi = R_1 \; if \; R_2^T \tag{31}$$

Here, R_1 and R_2 represent the produced polynomials and the face image. It is essential to highlight that the polynomial moment order determines the selection of the polynomial order. One can think of the generated moments (Φ) as a feature vector. The label of the matching face image ID is then appended to the feature vector. An array is created by combining all facial picture data in the database. The array is then normalized between -1 and 1 to guarantee that the features retain a constant dynamic range. SKTP and its hybrid versions, KP and TP, are evaluated for effectiveness and comparative analysis utilizing the AT&T facial database ORL. The database contains the faces of forty distinct persons. Each face image is 112×92 pixels in size. Ten photos of each person's face are taken at different times, with different lighting, expressions, and facial details. The RSVM model is trained using half of the face images during the training and testing phases. The moments taken from the data were used to train the RSVM model. The LIB-SVM was utilized to classify the data. RBF is employed in the RSVM model. Throughout the training phase, five-fold cross-validation was used to establish the gamma, cost and RSVM parameters. However, throughout the testing, various kinds of noise were added to every face image, making it challenging to assess SKTP's reliability. Three distinct forms of noise were employed during the degradation process: blur, salt and pepper, and Gaussian noise. Images without imperfections were utilized during the training phase exclusively. The classification accuracy is tested in the following ways to evaluate the classification's performance:

$$Accuracy = \frac{correctly\ predicted\ classes}{total\ testing\ classes} * 100\% \tag{32}$$

Ten separate testing and training images of faces were used for the testing and training stages to examine the stability of the categorization. The standard deviation and accuracy mean were computed for every ten iterations to evaluate the model's performance. Fig. 6 shows the separate training and testing phases in the face recognition system in this work.

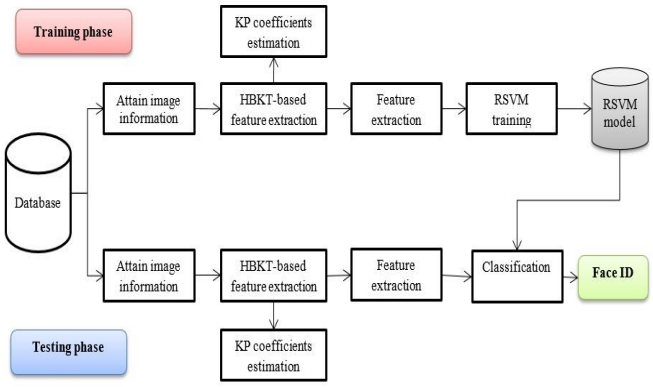

Fig. 6. Training and testing phases of the face recognition system.

G. Authentication

The evaluation of several continuous authentication systems presented in earlier research has yet to use various design criteria. A few studies consider limited requirements, such as accuracy and cost. Still, there needs to be a set of requirements for design that a continuous authentication system has to meet.

1) Passiveness: A system that is easy to operate shouldn't need constant user intervention. For instance, the user may find it very frustrating if the authentication system frequently requests that they re-enter their credentials.

2) Availability: A reliable authentication mechanism should always be available via the system. One major disadvantage of many previously suggested continuous authentication systems is that they are only sometimes available; they frequently fail because of insufficient data. In certain instances, a keyboard-centric system may erroneously decline access to a user engaged in movie viewing and not actively utilizing the keyboard.

3) High accuracy: High accuracy is, without question, the most crucial criterion for any authentication system. When a user attempts to log in as someone else, the system ought to be able to reliably and accurately identify them as imposters and deny their requests.

4) Scalability: With more users, the system should be able to manage an increasing volume of work. Its complexity in

terms of time and space should progressively increase with the number of users.

5) Efficiency: For two reasons, it is highly preferred to have a low response time or the amount of time needed to gather a test sample, analyze it, and render a conclusion. To promote user convenience, it is essential that the system rejects imposters and immediately authenticates legitimate users. Second, if there is a noticeable delay, security can also suffer. In the scenario where the authorization process requires five minutes, there is a potential vulnerability for an unauthorized individual to exploit the system and gain access to restricted resources during the on-going processing period, which lasts five minutes.

6) Low cost: The cost is a significant consideration regarding authentication methods used in low-security settings, like home computers. An authentication system should ideally be inexpensive to implement or alter in such contexts. Thus, systems without extra peripherals, like retina scanners, would often be preferred. However, expensive authentication systems could be used in highly secure areas like military bases.

7) Stability: Ideally, a feature should only slightly vary or retain its pattern for a specific time before being recorded for processing to facilitate authentication.

8) Extensibility: It should be possible for the authentication system to work on a broad range of devices independent of the underlying technology. No specific hardware should be needed for the system. One benefit of password-based authentication is its extensibility, which protects numerous methods, devices, and resources with limited system modification.

V. Results and Discussion

The proposed approach of remote user authentication based on face recognition is implemented in Python. The proposed work's environment is defined in Table I for when the face recognition based remote biometric user authentication system is implemented in real time on a login server.

After that, this work reviews five metrics employed to evaluate the suggested authentication system's accuracy. Traditionally, authentication systems are examined using the first three. To explore the precision of continuous authentication, we introduce two additional variables.

A. Metrics

The following metrics will be used in analyzing the results of applying the proposed method for face detection to perform facial user authentication in a remote biometric user authentication system:

1) False acceptance rate (FAR): The percentage of illegal users who are inadvertently approved in continuous authentication as opposed to the total number of fraudulent login attempts is known as the "False Acceptance Rate" (FAR). We use the notation $FAR_t = T_{EW}$ to describe the FAR below a given threshold, TEW. When security is the primary priority, it is advised to have a lower FAR.

2) False Rejection Rate (FRR): This indicator shows the percentage of legitimate requests mistakenly denied by users who have been granted authorized access to the system. The false rejection rate (FRR), when TEW is met, is shown by the notation $FRR_t = T_{EW}$. Because it improves user convenience, a lower FRR is preferred.

3) Rejection Rate (RR): This typically represents the total number of rejections (both legitimate and illegitimate) over the total number of attempts. In the context of authentication systems, this would mean how often access attempts are denied, regardless of whether those attempts are valid or invalid. RR Relationship to FRR (False Rejection Rate): The FRR is a subset of the RR, specifically focusing on the rate at which legitimate attempts (i.e., from authorized or genuine users) are incorrectly rejected. In contrast, RR could include all rejections, making it a broader measure. While FRR is a measure of system accuracy in identifying valid users, RR provides an overall view of the system's strictness or leniency in granting access.

4) Equal Error Rate (EER): Currently, it is noted that FAR and FRR are equivalent. However, because there is a trade-off between the two measurements, reporting FAR or FRR alone does not provide a complete picture. One rate can be lowered while permitting the other to rise. Therefore, we use EER (Equal Error Rate) rather than FAR or FRR to appropriately report the accuracy of H-RSVM (Context-Aware Behavior Analysis). This work uses $EER_t = T_{EW}$ notation to represent EER under TEW (Threshold Equal Weighting).

TABLE I. Recommended Login Server Hardware and Software Requirement

Requirements		
Sl. No	**Type**	**Specifications**
1	Processor	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz 2.99 GHz processor (minimum hardware requirement)
2	Storage	195 GB (minimum storage requirement)
3	RAM	8.00 GB (minimum RAM requirement)
4	Display	Monitor resolution 1024x768 (minimum resolution requirement)
		Software Requirements
Sl. No	**Software type**	**Specification**
1	OS	Windows 10 Pro (or later)
2	S/W	Python (version 3.0 or later)

5) False Acceptance Worst-case interval (FAW): Within a specific time-frame, T, the authentication system generates accept/reject decisions as its output. Two potential output patterns can occur when an impostor attempts to authenticate in a ten-minute authentication period. Both sequences exhibit an equal number of incorrect authorizations. However, the second sequence is deemed more problematic as the impostor can exploit the system for a continuous duration of four minutes without being detected. It is a decline from the first sequence, in which the impostor was limited to one minute of system use. The most significant amount of time (minutes) that a fraudulent user could be mistakenly identified as authentic is what we refer to as FAW. FAW equals one minute in the first case and four minutes in the second.

6) False Rejection Worst-case interval (FRW): In a similar manner to the concept of a False Acceptance Window (FAW), the notion of a False Rejection Window (FRW) is introduced, denoting the maximum duration (measured in minutes) during which an authorized user may be mistakenly rejected and misidentified as an impostor.

7) Scalability metrics: The complexity of the authentication system, in terms of space and time, will experience a gradual increase as the number of users grows, as previously discussed. We use the well-known O notation to show the space and time complexity of the H-RSVM technique as a function of N, the number of individuals in the dataset, to measure the scalability of the suggested method.

We used Python to create an H-RSVM prototype to examine the authentication system's accuracy. The correctness of the model is usually assessed with a different data point set than those used to construct it. Thus, the dataset is divided into training and test sets to aid creation and assessment. However, evaluating the efficacy of a system processing time series data is unsuitable for the conventional K-fold cross-validation approach. Time series data comprises a series of measurements that frequently show local relationships between observations. Cross-validation ignores the structural characteristics introduced in the data by these dependencies. Therefore, in this work, we devised many experimental scenarios to assess the authentication system's accuracy instead of utilizing conventional cross-validation. These circumstances are discussed next.

8) Baseline: The available dataset was split into two equal portions to create the baseline scenario, which resulted in $TEW = TRW = 7h$. The model was trained over the half dataset, which comprised the first seven hours for every subject, and was tested on the second half. All bio-streams ($n = 0,1,2,..$) were used for system testing and training. R-SVM-based classification technique is used. Both linear and Radial Basis Function (RBF) kernels were used in the SVM example. Our experimental results show that the testing error diminishes and approaches the minimum while the training error decreases and approaches zero as the number of repetitions grows. As a result, we have chosen to run 40 iterations across each classifier. This work has provided the $EER_t = 7h$ value for each classifier.

9) Biased FAR_t/FRR_t: While it is simple to evaluate authentication methods using EER_t, in situations where high security is required, we may need to restrict F RRt to enhance user convenience or minimize FAR_t to prevent impostors from gaining access. A low FAR_t indicates strong security, while a low FRR_t ensures user convenience. We employ the same settings as the baseline in this experimental configuration. It is important to note that false rejection and false acceptance have different consequences. We analyze two situations: (i) measuring FRR_t and attempting to minimize FAR_t and (ii) measuring FAR_t and attempting to minimize FRR_t. The results for these two scenarios are presented in Table II. Despite a higher FRR, Table II shows that H-RSVM prevents acceptance of impostors. Table II demonstrates that H-RSVM does not negatively impact user convenience, as it correctly rejects impostors over 90% of the time without mistakenly leaving legitimate users.

10) Variable window size: This work set the training and testing window sizes to seven hours over the baseline. In this instance, we modify the testing and training window lengths as the total of the two amounts equals fourteen hours, with the training window length ranging from two to twelve hours. The average equal error rate (EER_t) for several classifiers relative to the training window size is also illustrated. When we increase the training window size from two to six hours, EER_t significantly decreases for all classifiers. After that, it stays the same until TRW approaches 11h. There are two possible reasons why EER has started to increase over this TRW. First, an over-fitting of the model is possible. Secondly, there could not be enough test points.

11) Moving training window: We tested various values for TEW and TRW. Our experiments revealed that this verification approach achieved the most favourable outcome when TEW and TRW were set to 4 hours. With 15 nodes' tree size, the classification method used was R-SVM, and the average equal error rate (EER_t) was determined to be 1.9%. The trained model must remain valid for the successive four hours to achieve maximum accuracy for TRW.

Table II provides the false acceptance rate (FAR), equal error rate (EER), accuracy, precision, recall, F-measure, and false rejection rate (FRR) metrics for the proposed RSVM method as compared to other state-of-the-art methods for the three different datasets.

Fig. 7 shows the performance comparison of the metrics such as accuracy, precision, recall, and F-measure for the proposed H-RSVM method compared with the other state-of-the-art methods when the ORL dataset is used for model training.

Fig. 8 shows the performance comparison of the metrics such as accuracy, precision, recall, and F-measure for the proposed H-RSVM method compared with the other state-of-the-art methods when the GT dataset is used for model training.

TABLE II. COMPARISON OF PROPOSED MODEL WITH EXISTING APPROACHES

Dataset	Method	FAR	EER	Accuracy	Precision	Recall	F-Measure	FRR
ORL Dataset	RSVM	0.00094	0.0199	98.82%	98.23%	98.19%	98.21%	0.030
	KNN	0.0009	0.045	95.80%	95.89%	92.7%	94.3%	0.389
	DT	0.018	0.210	94.6%	92.8%	94.5%	93.6%	0.389
	RF	0.020	0.035	97.9%	96.8%	94.2%	94.4%	0.333
	CNN	0.052	0.032	98.8%	97.9%	96.3%	95.5%	0.
GT Dataset	RSVM	0.0014	0.0360	96.73%	96.16%	96.08%	96.12%	0.0692
	KNN	0.0014	0.055	96.0%	94.9%	92.8%	91.7%	0.356
	DT	0.019	0.220	93.6%	91.8%	91.7%	91.2%	0.399
	RF	0.021	0.045	96.9%	95.0%	92.4%	93.0%	0.393
	CNN	0.053	0.032	95.8%	95.8%	94.3%	93.5%	0.600
FACE94	RSVM	0.0005	0.0397	95.9%	95.83%	95.16%	95.49%	0.0784
	KNN	0.0005	0.045	95.0%	93.9%	91.7%	90.2%	0.349
	DT	0.021	0.210	92.6%	91.6%	90.7%	89.0%	0.389
	RF	0.023	0.035	95.9%	94.4%	92.4%	88.4%	0.833
	CNN	0.024	0.032	94.8%	93.9%	93.5%	92.0%	

TABLE III. RR, AUTHENTICATION DELAY, AND AUC COMPARISON WITH EXISTING APPROACHES

Rejection Rate (RR)	**ORL**	**GT**	**FACE94**
Proposed	0.9719	0.9407	0.9315
TPTSSR	0.9333	0.9233	0.9133
LPP	0.9357	0.9257	0.9057
CSDL-SRC	0.955	0.935	0.945
Deep CNN	0.91	0.901	0.900
SIFT	0.955	0.945	0.925
Authentication Delay (ms)	**ORL**	**GT**	**FACE94**
Proposed	1.3568	1.5405	1.4767
HMM-UBM	8	9	10
Conv-DCWRNN	15	16	17
AUC	**ORL**	**GT**	**FACE94**
Proposed	0.9804	0.97	0.95
DT	0.97	0.96	0.94
RF	0.92	0.91	0.90

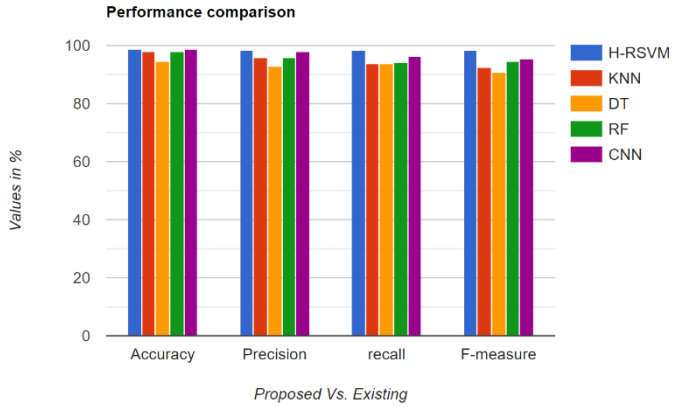

Fig. 7. Performance comparison with the ORL dataset.

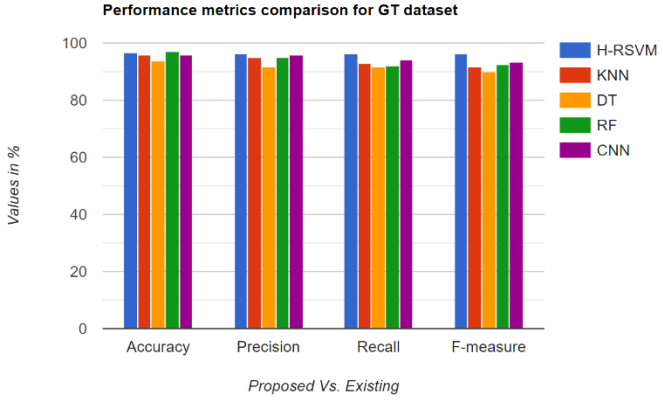

Fig. 8. Performance comparison with the GT dataset.

Fig. 9 shows the performance comparison of the metrics such as accuracy, precision, recall, and F-measure for the proposed H-RSVM method compared with the other state-of-the-art methods when the FACE94 dataset is used for model training.

Fig. 10 shows the performance comparison of other metrics such as FAR, EER, and FRR for the proposed H-RSVM method compared with the other state-of-the-art methods when the ORL dataset is used for model training.

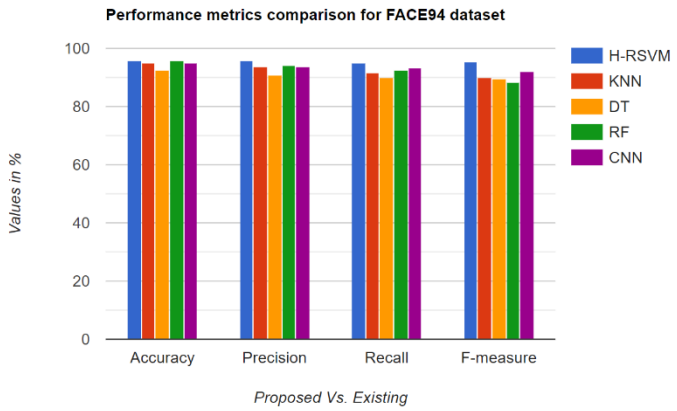

Fig. 9. Performance comparison with FACE94 dataset.

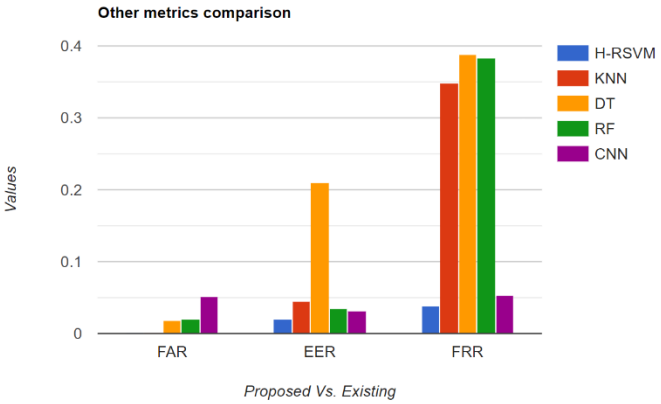

Fig. 10. Other metrics comparison with ORL dataset.

Fig. 11 shows the performance comparison of other metrics such as FAR, EER, and FRR for the proposed H-RSVM method compared with the other state-of-the-art methods when the GT dataset is used for model training.

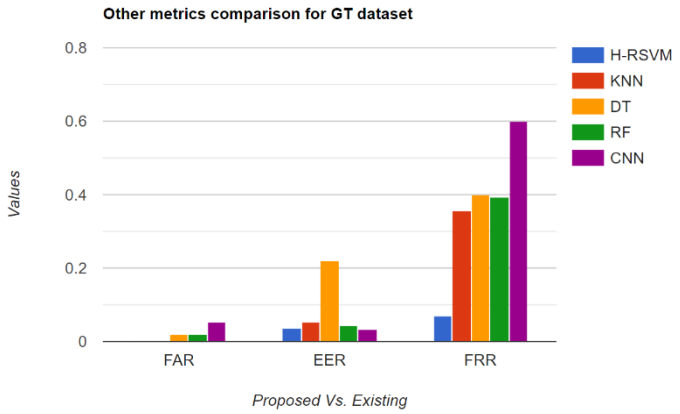

Fig. 11. Other metrics comparison with the GT dataset.

Fig. 12 shows the performance comparison of other metrics such as FAR, EER, and FRR for the proposed H-RSVM method compared with the other state-of-the-art methods when the FACE94 dataset is used for model training.

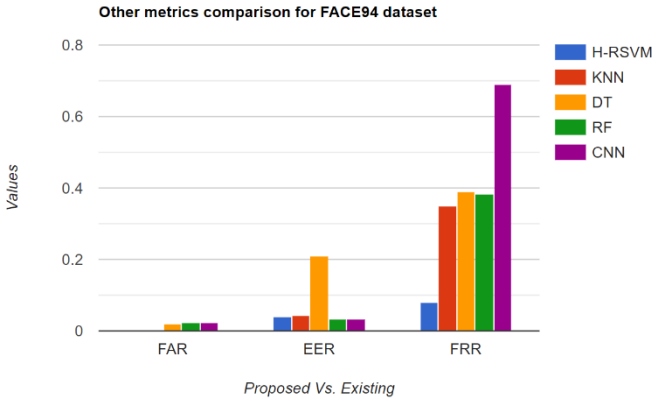

Fig. 12. Other metrics comparison with the FACE94 dataset.

Fig. 13 shows the performance comparison of another metric RR for the proposed H-RSVM method compared with other state-of-the-art methods for all datasets used in training.

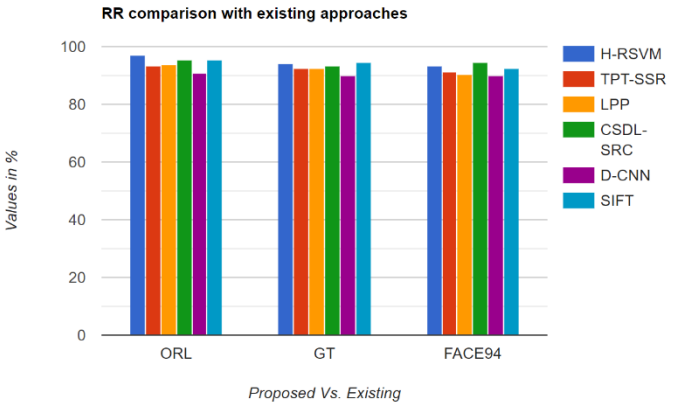

Fig. 13. RR comparison with existing approaches.

Fig. 14 shows the performance comparison of another metric, authentication delay, for the proposed H-RSVM method compared with the other state-of-the-art methods for all three datasets used for model training.

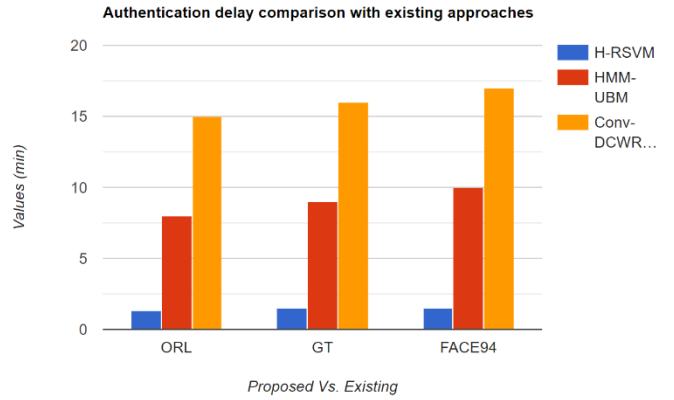

Fig. 14. Authentication delay comparison with existing approaches.

Fig. 15 shows the performance comparison of another metric, area under curve (AUC), for the proposed H-RSVM method compared with other state-of-the-art methods for all three datasets used for model training.

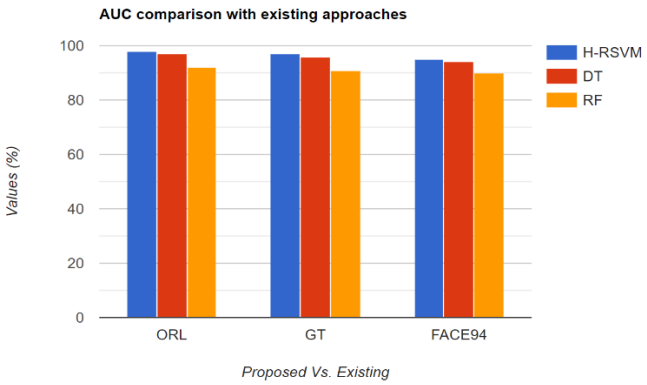

Fig. 15. AUC comparison with existing approaches.

Fig. 16 and Fig. 17 depict failed authentication and successful authentication use cases, respectively, using the proposed face-recognition-based remote authentication system. The model gives the correct prediction outcomes for both non-authorized user and authorized user with high rate of prediction accuracy. Based on the experimentation, it is proven that the anticipated model works well compared to other approaches, as discussed further below.

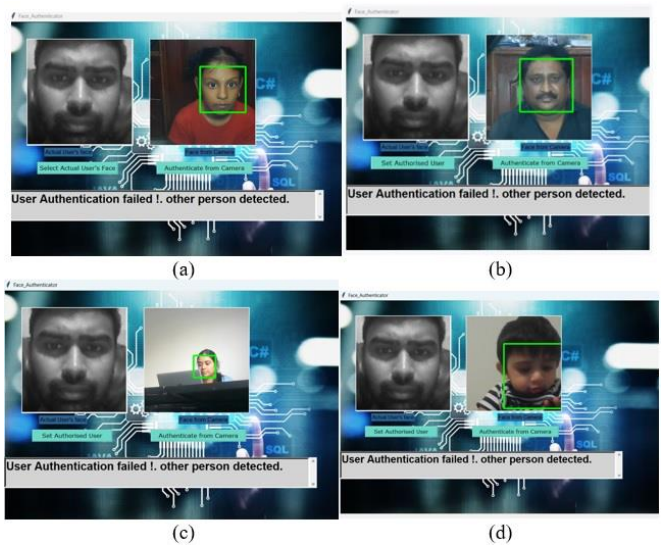

Fig. 16. Authentication outcomes for non-authorized users (a-d).

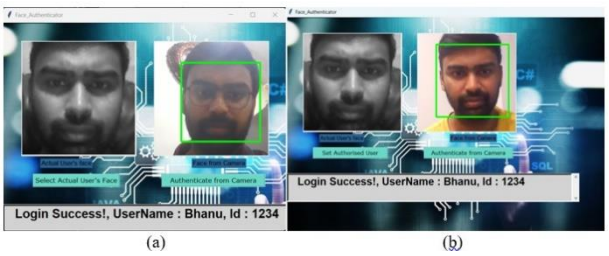

Fig. 17. Authentication outcomes for an authorized user (a-b).

Table II compares existing approaches like KNN, DT, RF and CNN. Metrics like FAR, EER, FRR, accuracy, precision, recall and F-measure are evaluated and compared. The proposed model gives 98.82% accuracy for the ORL dataset, 96.73% accuracy for the GT dataset, and 95.9% accuracy for the FACE94 dataset. The proposed model offers 98.23%, 96.16%, and 95.83% precision for the ORL, GT, and FACE94 datasets. It gives 98.19%, 96.08%, and 95.16% recall for ORL, GT, and FACE94 datasets. The proposed H-RSVM model gives 98.21%, 96.12%, and 95.49% F-measure for ORL, GT, and FACE94 datasets (see Fig. 7-12). Table III compares RR, authentication delay, and AUC evaluation with other approaches. The proposed model gives 98.04% AUC for ORL, 97% for GT, and 95% for the FACE94 dataset. The authentication delay is lesser for the proposed model, and the RR of the anticipated model is 97.19% for ORL, 94.07% for GT, and 93.15% for the FACE94 dataset, respectively (see Figures 13-15). Based on the observations, it is noted that the proposed model gives satisfying outcomes compared to other approaches.

B. Real-time Authentication

We define authorization at the outset of this section. Next, this work presents a real-time adaptive authorization (RAA) system that leverages H-RSVM's judgments to offer a tremendously flexible access control strategy. The RAA concept is not exclusive to H-RSVM. It provides a flexible model of access control that can be implemented in any authorization system that allows users to access content based on choices made by a continuous authentication method. Authorization determines whether to grant access to a system, resource, or location to a person who has already undergone authentication. Conventional authorization techniques use the user ID of an authenticated user to assign them a specific access level. However, as demonstrated by the non-zero FRR of continuous authentication systems, this simple method may unintentionally block allowed access if the authentication system cannot identify a legitimate user for a short time. Imagine a situation where a personal laptop is secured against unauthorized users using a continuous authentication method. The authentication technique authenticates the user at first. Using user ID, the authorization system establishes the user's access level. Nonetheless, the laptop can log users out if the authentication process unintentionally rejects them. The inconvenience resulting from false rejections can be reduced by using RAA techniques. These techniques continually adjust the user's access level following the authentication system's most recent determination. Here, we introduce an RAA technique with an ongoing authentication scheme.

A trust-based RAA modifies the user's access level in real-time using the trust level (TRL) parameter. Based on past choices made by the continuous authentication system, the recently established TRL metric measures our degree of confidence in a user. A higher number on the TRL scale, which ranges from 0 to 100, denotes a higher degree of trust. TRL has an initial value of 100 when a user is approved and authenticated. Following every user authentication, the trust update method continuously updates the TRL value. A simple technique for updating trust could involve increasing or decreasing TRL by a fixed amount following every accept or reject choice. The pseudo-code for this method is displayed in the trust update procedure. Two parameters, W_{accept} *and* W_{reject}, need to be set. When we are positive that a user is authentic, we should set the TRL value to 100. Otherwise, it has to be set to 0 immediately as we learn that an impostor exists. It indicates that the values of

W_{accept} *and* W_{reject} need to be chosen appropriately. In the worst-case situation, the authentication system can inadvertently deny three consecutive requests from legitimate users if, for instance, an SVM classifier with 15 nodes' tree size yields a false rejection rate of 3. The RAA approach concludes that a user is fraudulent ($TRL = 0$) if the authentication system rejects a request four times in a row. With this classifier, we can use the following formula to set the value of W_{reject}: $-100\ FRW + 1 = -100\ 4 = -25\ is\ W_{reject}.FAW = 4$ means that, in the worst situation, four successive tries would lead to mistakenly identifying an impostor as a valid user. TRL should be more prominent than 100 if the authentication system accepts five requests in a row. Therefore, the formula for setting W_{accept} is as follows: $W_{accept} = +100\ FAW + 1 = +100\ 5 = +20$. Various purposes may require different threshold levels to be specified. The work decided to restrict the threshold value for these accounts to 100 to ensure that the user can evaluate input images when the system is positive they are real. However, a lesser degree of trust might be adequate for less sensitive activities, like basic web browsing. When combined with RAA, H-RSVM can improve user-friendliness without compromising the high-security standards required for critical applications.

VI. Conclusion and Future Work

This work develops a continuous remote biometric user authentication system based on a face recognition model pre-trained on face image datasets. This research work implements an algorithm combining HB-KT Polynomials and RSVM for a face recognition based remote user authentication system that implements a model pre-trained on the ORL, Face94 and GT datasets to perform face recognition for continuous remote biometric user authentication. Comprehensive analysis has been performed to ascertain the accuracy and performance of the proposed method as compared to previous state-of-the-art algorithms. A functioning prototype has also been implemented as a Python program. The proposed model gives accuracies of 98.82% (ORL dataset), 96.73% (GT dataset), and 95.9% (Face94 dataset). Compared to other previous state-of-the-art models, the proposed model generally has been observed to have higher F-measure, accuracy, and speed. More research should be made on the use of multimodal biometric data, taken from multiple channels including face recognition, voice, and behavioral characteristics to improve the performance of continuous user authentication. Developing adaptive machine learning algorithms tailored for user interfaces that can produce personalized methods based on the particular interaction can help consider the change in behavior depending on context or mood. Privacy related issues need to be resolved, which requires storage and processing to be secure and possible solutions include decentralized approaches or homomorphic encryption. Moreover, context aware computing can adapt the authentication requirements depending on the ongoing situation context factors, usability studies are vital for the assessment of users' acceptance and interaction with the established systems, ensures both secure and usability.

Acknowledgment

This research was performed at Texas A&M University-Kingsville in a project funded by the Department of Homeland Security (DHS) through the grant no. 21STSLA00011-01-00. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

References

[1] S. Saragih, J. Lucey, and J. Cohn, "Deformable model fitting by regularized landmark mean-shifts," Int. J. Comput. Vis., vol. 91, pp. 200–215, 2010.

[2] T. Sujatha, N.R. Wilfred Blessing, S. Anand, and E. Daniel, "Automated face authentication and recognition using deep neural network with SVM classifier in cloud environment," in *Disruptive Technologies for Big Data and Cloud Applications*, J.D. Peter, S.L. Fernandes, and A.H. Alavi, Eds., vol. 905, Springer, Singapore, 2022.

[3] L. Liu, W. Ouyang, X. Wang, P. Fieguth, J. Chen, X. Liu, and M. Pietikainen, "Deep learning for generic object detection: a survey," *arXiv preprint arXiv:1809.02165*, 2018.

[4] S. Xie, R. Girshick, P. Dollar, Z. Tu, and K. He, "Aggregated residual transformations for deep neural networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, pp. 1492–1500, 2017.

[5] R.J. Wang, X. Li, and C.X. Ling, "Pelee: a real-time object detection system on mobile devices," in *Advances in Neural Information Processing Systems*, pp. 1963–1972, 2018.

[6] L. Li, X. Feng, Z. Xia, et al., "Face spoofing detection with local binary pattern network," *J. Vis. Commun. Image Represent.*, pp. 182–192, 2018.

[7] S. Ren, K. He, R. Girshick, et al., "Faster R-CNN: towards real-time object detection with region proposal networks," in *Advances in Neural Information Processing Systems*, pp. 91–99, 2015.

[8] J. Redmon, S. Divvala, R. Girshick, et al., "You only look once: unified real-time object detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, pp. 779–788, 2016.

[9] M. Ramgopal, M.S. Roopesh, M.V. Chowdary, et al., "Masked facial recognition in security systems using transfer learning," *SN Comput. Sci.*, vol. 4, p. 27, 2023.

[10] J. Imran and B. Raman, "Deep motion templates and extreme learning machine for sign language recognition," *Vis. Comput.*, 2019.

[11] S. Ravi, M. Suman, P.V.V. Kishore, K. Kumar, and A. Kumar, "Multi-modal spatio-temporal co-trained CNNs with single modal testing on RGB–D based sign language gesture recognition," *J. Comput. Lang.*, vol. 52, pp. 88–102, 2019.

[12] G. Hu, Y. Yang, D. Yi, J. Kittler, W. Christmas, S.Z. Li, and T. Hospedales, "When face recognition meets with deep learning: An evaluation of convolutional neural networks for face recognition," in *Proc. IEEE Int. Conf. Comput. Vis. Workshops*, Santiago, Chile, pp. 142–150, 2015.

[13] P.S. Prasad, R. Pathak, V.K. Gunjan, and H.V.R. Rao, *Deep Learning Based Representation for Face Recognition*. Springer, Berlin, Germany, pp. 419–424, 2019.

[14] Y. Liu, M. Lin, W. Huang, and J. Liang, "A physiognomy-based method for facial feature extraction and recognition," *J. Vis. Lang. Comput.*, vol. 43, pp. 103–109, 2017.

[15] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Columbus, OH, USA, pp. 1701–1708, 2014.

[16] K. He, X. Zhang, S. Ren, and J. Sun, "Spatial pyramid pooling in deep convolutional networks for visual recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 37, pp. 1904–1916, 2015.

[17] J. Yu, K. Sun, F. Gao, and S. Zhu, "Face biometric quality assessment via light CNN," *Pattern Recognit. Lett.*, vol. 107, pp. 25–32, 2018.

[18] R. Singh and H. Om, "Newborn face recognition using deep convolutional neural network," *Multimed. Tools Appl.*, vol. 76, pp. 19005–19015, 2017.

[19] Y. Sun, X. Wang, and X. Tang, "Hybrid deep learning for computing face similarities," *Int. Conf. Comput. Vis.*, vol. 38, pp. 1997–2009, 2013.

[20] G.P. Nam, H. Choi, and J. Cho, "PSI-CNN: A pyramid-based scale-invariant CNN architecture for face recognition robust to various image resolutions," *Appl. Sci.*, vol. 8, p. 1561, 2018.

[21] D. Menotti, G. Chiachia, A. Pinto, W.R. Schwartz, H. Pedrini, A.X. Falcao, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, pp. 864–879, 2015.

[22] C. Qin, X. Lu, P. Zhang, H. Xie, and W. Zeng, "Identity recognition based on face image," *J. Phys. Conf. Ser.*, vol. 1302, p. 032049, 2019.

[23] Z. Zhu, P. Luo, X. Wang, and X. Tang, "Recover canonical-view faces in the wild with deep neural networks," *arXiv preprint arXiv:1404.3543*, 2014.

[24] Z. Lu, X. Jiang, and A.C. Kot, "Deep coupled ResNet for low-resolution face recognition," *IEEE Signal Process. Lett.*, vol. 25, pp. 526–530, 2018.

[25] Y. Zhang, D. Zhao, J. Sun, G. Zou, and W. Li, "Adaptive convolutional neural network and its application in face recognition," *Neural Process. Lett.*, vol. 43, pp. 389–399, 2016.

[26] B. Abd El-Rahiem, M. Amin, A. Sedik, F.E. Abd El Samie, and A.M. Iliyasu, "An efficient multi-biometric cancellable biometric scheme based on deep fusion and deep dream," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 4, pp. 2177–2189, 2022.

[27] A. Rengaraj, A.R. Kishan, A. Abraham, and A. Sattenapalli, "Centralized intelligent authentication system using deep learning with deep dream image algorithm," in *Advances in Power Systems and Energy Management*, Springer, Singapore, pp. 169–178, 2021.

[28] E.A. Elshazly, F.G. Hashad, A. Sedik, and N. Abdel-Salam, "Compression-based cancelable multi-biometric system," *Research Square*, Nov. 2022.

[29] D. Lu and L. Yan, "Face detection and recognition algorithm in digital image based on computer vision sensor," *J. Sensors*, vol. 2021, pp. 1–16, Sep. 2021.

[30] H.R. Vijaya Kumar and M. Mathivanan, "A novel hybrid biometric software application for facial recognition considering uncontrollable environmental conditions," *Healthcare Anal.*, vol. 3, 2023.

[31] S. Hangaragi, T. Singh, and N. Neelima, "Face detection and recognition using face mesh and deep neural network," *Procedia Comput. Sci.*, vol. 218, pp. 741–749, 2023.

[32] R. Sharma and A. Ross, "Periocular biometrics and its relevance to partially masked faces: A survey," *Comput. Vis. Image Underst.*, vol. 226, 2023.

[33] G. Rajeshkumar, M. Braveen, R. Venkatesh, P. Josephine Shermila, B. Ganesh Prabu, B. Veerasamy, B. Bharathi, and A. Jeyam, "Smart office automation via faster R-CNN based face recognition and internet of things," *Measurement: Sensors*, vol. 27, p. 100719, 2023.

[34] J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, "An investigation of biometric authentication in the healthcare environment," *Array*, vol. 8, 100042, 2020.

[35] A. Saini, "Analysis of different face recognition algorithms," *Int. J. Eng. Res. Technol.*, vol. 3, no. 11, pp. 235–239, 2014.

[36] "Cambridge ORL Face Database," available at: https://cam-orl.co.uk/facedatabase.html.

[37] "AT&T Lab. Cambridge Face Database," available at: www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.